LEGISLATIVE AUDITS

REPORT FOLLOW-UP

AGENCY: IDAHO DEPARTMENT OF FISH AND GAME

On September 6, 2007, the Legislative Services Office released a Management Report for the Idaho Department of Fish and Game for fiscal years 2004, 2005, and 2006. The Department was contacted on January 31, 2008, and this follow-up report addresses how the Department has responded to the two findings and recommendations contained in that report.

STATUS OF RECOMMENDATIONS:

FINDING #1 – Purchasing rules were not followed on information technology projects.

We recommended that the Department follow purchasing rules. Additional staff training and communication may be needed to ensure compliance with purchasing rules.

AUDIT FOLLOW-UP – The Department has increased its contract reviews and has provided accounts payable with a list of approved contracts authorized for payment. The Department is working on updating its purchasing policy and is providing ongoing training to staff.

STATUS – CLOSED

FINDING #2 – Sensitive personal and financial data of customers is not properly safeguarded.

We recommended that the Department develop a comprehensive approach for safeguarding sensitive personal and financial data of customers. This effort should include identifying each location where data is stored, both electronic and hard copy formats, and appropriate technologies or other measures to safeguard this data from unauthorized access. We also recommended that the Department develop procedures for monitoring, investigating, and promptly notifying customers if data has been breached.

AUDIT FOLLOW-UP – The Department's new point of sale system is encrypted and includes various firewalls to protect data in transit. Encryption is currently being used on all outside data transfers and has also been made available for desktops, laptops, and handheld devices. The official training on how to best utilize it will be completed this spring. The Department has also obtained a draft security breech notification policy from ITRMC, and is reviewing this document to determine how to integrate this policy with its systems. Physical security of hard copy sensitive data has been secured through the use of locked shred boxes and storage cabinets.

STATUS: OPEN